Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A computer-implemented method for managing access to electronic documents, comprising:

associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the encrypted document, the first key being usable to decrypt the encrypted document decryption key; and

providing the first key in an access controlled manner to users for use in opening the encrypted document.

2. (Currently amended) The method of claim 1, further comprising:

storing the encrypted document decryption key in the encrypted document.

3. (Original) The method of claim 1, further comprising:

encrypting the first key;

associating with the encrypted first key a second key that can be used to decrypt the encrypted first key; and

providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the first key.

4. (Original) The method of claim 1, further comprising:

providing a second encrypted document decryption key for a second encrypted document, the second encrypted document decryption key when decrypted yielding a document decryption

key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the first key is usable to decrypt the second encrypted document decryption key; and

associating the first key with the second encrypted document decryption key.

5. (Original) The method of claim 4, further comprising:

providing a third encrypted document decryption key for the second encrypted document, the third encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the third encrypted document decryption key being encrypted so that a third key is usable to decrypt the third encrypted document decryption key;

associating the third key with the third encrypted document decryption key; and

providing the third key in an access controlled manner to users for use in opening the second document.

6. (Original) The method of claim 3, further comprising:

associating a third key with a second encrypted document decryption key for a second document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the third key is usable to decrypt the second encrypted document decryption key.

7. (Original) The method of claim 6, further comprising:

encrypting the third key;

associating the second key with the encrypted third key, the second key being usable to decrypt the encrypted third key; and

providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the third key.

8. (Original) The method of claim 1, wherein providing the first key in an access controlled manner comprises sending the first key to users in rights management information specific to systems of the users to whom the first key is sent.

9. (Original) The method of claim 8, wherein the rights management information comprises a rights management file.

10. (Original) The method of claim 1, wherein providing the first key in an access controlled manner comprises sending information used to synthesize the first key in rights management information.

11. (Original) The method of claim 3, wherein associating further comprises:
storing the encrypted first key in rights management file information for the first key.

12. (Original) The method of claim 11, further comprising:
associating a unique identifier with the second key;
and storing the unique identifier in the rights management information with the encrypted first key.

13. (Original) The method of claim 1, further comprising:
providing a document decryption key in an access controlled manner to users for accessing the document without using the first key.

14. (Original) The method of claim 2, further comprising:
associating a unique identifier with the first key.

15. (Original) The method of claim 14, wherein the unique identifier is stored in the document in association with the encrypted document decryption key to associate the first key with the encrypted document decryption key.

16. (Original) The method of claim 10, wherein the rights management information provides a license and defines a set of permission rights associated with the license.

17. (Original) The method of claim 16, wherein the set of permission rights specifies a right allowing another key to be associated with the rights management information so that a holder of such a key has access to the first key.

18. (Original) The method of claim 16, wherein the set of permission rights specifies a right allowing a holder of the first key to add to a second encrypted document a second encrypted document decryption key that can be decrypted by the first key and, when decrypted by the first key, yielding a second document decryption key that is usable to decrypt the encrypted second document.

19. (Original) The method of claim 16, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.

20. (Original) The method of claim 19, wherein the rights management information comprises a rights management file.

21. (Original) The method of claim 19, wherein the rights management file is specific to a particular user.

22. (Original) The method of claim 19, wherein the rights management file is specific to a particular user-operated system.

23. (Original) The method of claim 1, wherein the encrypted document decryption key is encrypted by an encryption key that is different from the first key.

24. (Original) The method of claim 23, wherein the first key is a public key and the encryption key is a private key.

25. (Original) The method of claim 24, wherein providing the first key in an access controlled manner comprises sending information used to synthesize the first key in a rights management file and wherein the rights management file enables access to the private key.

26. (Currently amended) A computer-implemented method for accessing an electronic document, comprising:

obtaining an encrypted electronic document;

obtaining a collection of keys, the keys including keys that are encrypted, the keys and the document having associations defined between certain pairs of them, where each association of a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection;

using the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access.

27. (Original) The method of claim 26, wherein the associations are represented as a directed graph, with each node representing a key or the document, with one or more nodes representing keys accessible to the user, and with one or more edges pointing to the document, and wherein using the associations to identify at least one key comprises:

finding a path in the directed graph to the node representing the document from one of the nodes representing keys accessible to the user.

28. (Original) The method of claim 27, further comprising:

following the path and decrypting each of the keys represented by nodes along the path in turn until an encrypted document decryption key for the document is decrypted.

29. (Original) The method of claim 28, wherein each encrypted key is identified by two IDs, including a first ID corresponding to the encrypted key and a second ID corresponding to another of the keys capable of decrypting the encrypted key.

30. (Original) The method of claim 29, wherein two or more second IDs correspond to the same first ID, and each of the two or more second IDs and the encrypted keys to which they correspond are stored as separate entries in an array of entries, each of the entries being indexed by the same first ID.

31. (Original) The method of claim 29, wherein each encrypted key is stored with the corresponding second ID as an entry in an array and each entry is indexed by the corresponding first ID.

32. (Currently amended) A computer-implemented method for managing access to encrypted electronic documents, comprising:

providing in an access controlled manner multiple skeleton decryption keys for multiple encrypted documents, where a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys;

each single skeleton key being a key usable to decrypt one or more secondary decryption keys; and

each secondary decryption key being a skeleton key or a decryption key for an encrypted document;

whereby one or more skeleton keys can be issued for a document or a set of documents, and a holder of a particular skeleton key can open any document to which the particular skeleton key applies, directly or indirectly.

33. (Original) The method of claim 32, wherein the skeleton keys are distributed to users in rights management files.

34. (Currently amended) A computer program product, tangibly embodied on a machine-readable medium ~~or propagated signal~~, for managing access to encrypted electronic documents, comprising instructions operable to cause a programmable processor to:

associate a first key with an encrypted document decryption key, the encrypted document decryption key being associated with a document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the document, the first key being usable to decrypt the encrypted document decryption key; and

provide the first key in an access controlled manner to users for use in opening the document.

35. (Currently amended) A computer program product, tangibly embodied on a machine-readable medium ~~or propagated signal~~, for accessing an electronic document, comprising instructions operable to cause a programmable processor to:

obtain an encrypted electronic document;

obtain a collection of keys, the keys including keys that are encrypted, the keys and the document having associations defined between certain pairs of them, where each association of a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection; and

use the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access.

36. (Currently amended) A computer program product, tangibly embodied on a machine-readable medium ~~or propagated signal~~, for managing access to encrypted electronic documents, comprising instructions operable to cause a programmable processor to:

provide in an access controlled manner multiple skeleton decryption keys for multiple

encrypted documents, where a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys;

each single skeleton key being a key usable to decrypt one or more secondary decryption keys; and

each secondary decryption key being a skeleton key or a decryption key for an encrypted document;

whereby one or more skeleton keys can be issued for a document or a set of documents, and a holder of a particular skeleton key can open any document to which the particular skeleton key applies, directly or indirectly.

37. (New) The method of claim 1, wherein the set of permission rights specifies a right allowing a holder of the first key to add to a second encrypted document a second encrypted document decryption key that can be decrypted by the first key and, when decrypted by the first key, yielding a second document decryption key that is usable to decrypt the encrypted second document.

38. (New) The method of claim 1, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.